



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,434	11/28/2003	David Lawler Christiansen	MS1-1703US	1238
22801	7590	12/10/2008		
LEE & HAYES, PLLC 601 W. RIVERSIDE AVENUE SUITE 1400 SPOKANE, WA 99201			EXAMINER MEYERS, MATTHEW S	
			ART UNIT 3689	PAPER NUMBER
			MAIL DATE 12/10/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/724,434

Applicant(s)

CHRISTIANSEN, DAVID LAWLER

Examiner

MATTHEW S. MEYERS

Art Unit

3689

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/5508)
- Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is in response to applicant's communication on 11/28/2003, wherein claims 1-27 are currently pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has used the term "substantially". It is unclear as to what this term comprises.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-12 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In order for a method to be considered a "process" under §101, a claimed process must either: (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials). *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972). If

neither of these requirements is met by the claim, the method is not a patent eligible process under §101 and is non-statutory subject matter. With respect to claims 1-12, the claim language does not include the required tie or transformation and thus is directed to nonstatutory subject matter.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claims 1-27 are rejected under 35 U.S.C. 102(a) as being anticipated by *How Security Descriptors and Access Control Lists Work*, Microsoft® TechNet, Updated March 28 , 2003 (Hereinafter referred to as Technet).

8. With respect to **Claim 1**:

9. Technet discloses a computer-executable method, comprising:

a. intercepting a message that modifies security information associated with an object, the security information identifying an owner of the object and an entity that has access to the object (Technet, Page 18, "The canonical order also ensures that all explicit ACEs are processed before any inherited ACE. This is consistent with the concept of discretionary access control: access to a child object is at the discretion of the child's owner, not the parent's owner.");

- b. determining if the owner exceeds a first threshold security level, and if so, issuing a first notification that the owner exceeds the threshold security level (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal."); and
 - c. determining if the entity that has access to the object exceeds a second threshold security level, and if so, issuing a second notification that the entity exceeds the second threshold security level ((Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").
10. With respect to **Claim 2**:
11. Technet discloses wherein the first threshold security level identifies the owner as being a questionable security risk (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE

identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

12. With respect to **Claim 3**:

13. Technet discloses wherein the first threshold security level identifies the owner as being a dangerous security risk (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

14. With respect to **Claim 4**:

15. Technet discloses wherein not exceeding the first threshold security level identifies the owner as being trusted (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

16. With respect to **Claim 5**:

17. Technet discloses determining if a grant of permissions to the entity exceeds a third security threshold, and if so, issuing a third notification that the grant of permissions exceeds the third security threshold (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

18. With respect to **Claim 6**:

19. Technet discloses wherein the grant of permissions comprises information that describes what access to the object for which the entity is authorized (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

20. With respect to **Claim 7**:

21. Technet discloses wherein the security information is embodied in a security descriptor associated with the object (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

22. With respect to **Claim 8**:

23. Technet discloses wherein the security descriptor further comprises an owner field having a security identifier that identifies a security context associated with the owner (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

24. With respect to **Claim 9**:

25. Technet discloses wherein the security descriptor further comprises a Discretionary Access Control List containing the information about the entity that has access to the object (Technet, Page 10, "An ACL is an ordered list of ACEs that define

the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

26. With respect to **Claim 10**:

27. Technet discloses wherein the information about the entity comprises a security identifier that identifies a security context of the entity, and an access mask that defines permissions granted to the entity (Technet, Page 11, “When a thread tries to access a securable object, the system either grants or denies access. If the object does not have a DACL, the system grants access; otherwise, the system looks for ACEs in the object’s DACL that apply to the thread. Each ACE in the object’s DACL specifies the access rights that are allowed or denied for a security principal or logon session.”).

28. With respect to **Claim 11**:

29. Technet discloses wherein intercepting the message comprises hooking an Application Programming Interface (API) that enables the modification to the security information (Technet, Page 3, “Security Descriptor Control Flags”).

30. With respect to **Claim 12**:

31. Technet discloses a computer-readable medium having computer-executable instructions for performing the method recited in claim 1 (Technet, Page 1, “The access control model that is used by the Windows Server 2003 operating system is administered at the object level by setting different levels of access, or permissions, to objects.”).

32. With respect to **Claim 13**:

33. Technet discloses a computer-readable medium having computer-executable instructions for evaluating a security threat posed by an application modifying an object, the instructions comprising:

- d. intercepting a modified security descriptor for an object, the security descriptor including an owner SID field and a DACL, the owner SID field identifying an owner of the object, the DACL identifying at least one entity that has access to the object and access permissions for the entity (Technet, Page 18, "The canonical order also ensures that all explicit ACEs are processed before any inherited ACE. This is consistent with the concept of discretionary access control: access to a child object is at the discretion of the child's owner, not the parent's owner.");
- e. evaluating the owner of the object to determine if the owner is categorized as dangerous, and if so, issuing an alert notification (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.");
- f. evaluating the DACL to determine if the entity is categorized as dangerous, and if so, issuing the alert notification (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control

access to an object. When an audited action occurs, the operating system records the event in the security log.” and Page 10, “An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”); and

g. if the entity is not categorized as trusted, evaluating the DACL to determine if the access permissions for the entity are categorized as dangerous, and if so, issuing the alert notification (Technet, Page 3, “The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log.” and Page 10, “An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

34. With respect to **Claim 14**:

35. Technet discloses evaluating the owner of the object to determine if the owner is categorized as questionable, and if so, issuing a warning notification (Technet, Page 3, “The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log.” and Page 10, “An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies

a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

36. With respect to **Claim 15**:

37. Technet discloses evaluating the DACL to determine if the entity is categorized as questionable, and if so, issuing a warning notification (Technet, Page 3, “The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log.” and Page 10, “An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

38. With respect to **Claim 16**:

39. Technet discloses evaluating the DACL to determine if the access permissions are categorized as questionable, and if so, issuing a warning notification (Technet, Page 3, “The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log.” and Page 10, “An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.”).

40. With respect to **Claim 17**:

41. Technet discloses wherein the notification comprises a substantially instantaneous notice issued to a user (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

42. With respect to **Claim 18**:

43. Technet discloses wherein the notification comprises an entry in a log (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

44. With respect to **Claim 19**:

45. Technet discloses a computer-readable medium having computer-executable components, comprising:

- h. a security verifier having a security descriptor evaluator component configured to intercept a message that affects security information of an object, and to evaluate a security identifier associated with an entity having access rights

to the object, the evaluation including a determination whether the entity is categorized as other than trusted, the security descriptor evaluator component being further configured to issue a notification if the entity is categorized as other than trusted (Technet, , Page 18, "The canonical order also ensures that all explicit ACEs are processed before any inherited ACE. This is consistent with the concept of discretionary access control: access to a child object is at the discretion of the child's owner, not the parent's owner.", Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

46. With respect to **Claim 20**:

47. Technet discloses wherein the security descriptor evaluator component is further configured to issue a second notification if the entity is categorized as dangerous (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

48. With respect to **Claim 21**:

49. Technet discloses wherein the security descriptor evaluator component is further configured to evaluate a second security identifier associated with an owner of the object, and to issue a notification if the owner is categorized as other than trusted (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

50. With respect to **Claim 22**:

51. Technet discloses wherein the security descriptor evaluator component is further configured to issue a second notification if the owner is categorized as dangerous (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

52. With respect to **Claim 23**:

53. Technet discloses wherein the security descriptor evaluator component is further configured to evaluate the access rights of the entity, and to issue a notification if the

access rights are categorized as other than safe (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

54. With respect to **Claim 24**:

55. Technet discloses wherein the security descriptor evaluator component is further configured to issue a second notification if the access rights are categorized as dangerous (Technet, Page 3, "The SACL is similar to the DACL except that the SACL is used to audit rather than control access to an object. When an audited action occurs, the operating system records the event in the security log." and Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

56. With respect to **Claim 25**:

57. Technet discloses wherein the security information is contained in a security descriptor associated with the object (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

58. With respect to **Claim 26**:

59. Technet discloses wherein the security identifier is contained within a DACL (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

60. With respect to **Claim 27**:

61. Technet discloses wherein the access rights are described in the DACL (Technet, Page 10, "An ACL is an ordered list of ACEs that define the protections that apply to an object and its properties. Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.").

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW S. MEYERS whose telephone number is (571)272-7943. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jan Mooneyham can be reached on (571) 272-6805. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew S. Meyers/
Examiner, Art Unit 3689

/Janice A. Mooneyham/
Supervisory Patent Examiner, Art Unit 3689